

AMENDMENTS TO THE CLAIMS

1 1. (currently amended) A method for providing secure external memory that stores
2 instructions for a processor, comprising the steps of:

3 receiving a plurality of encrypted instructions into a buffer of the processor from
4 the external memory, said plurality of encrypted instructions comprise a plurality of consecutive
5 encrypted instructions, and said step of receiving said plurality of encrypted instructions into a
6 buffer of the processor from the external memory comprises the step of receiving the plurality of
7 consecutive encrypted instructions from a bus having a width equivalent to that of each
8 consecutive encrypted instruction of the plurality of consecutive encrypted instructions;

9 decrypting the plurality of encrypted instructions substantially simultaneously
10 using a selected decryption algorithm to produce a plurality of decrypted instructions; and

11 forwarding at least one decrypted instruction of the plurality of decrypted
12 instructions to a processing area of the processor.

1 2. (canceled)

1 3. (canceled)

1 4. (original) The method according to claim 3, wherein the width is equal to eight (8) bits.

1 5. (original) The method according to claim 1, wherein the selected decryption algorithm
2 comprises at least one of a data encryption standard (DES), a triple DES, and an advanced
3 encryption standard (AES).

1 6. (currently amended) A method for providing secure external memory that stores
2 instructions for a processor, comprising the steps of: ~~The method according to claim 1,~~
3 receiving a plurality of encrypted instructions into a buffer of the processor from
4 the external memory;

5 decrypting the plurality of encrypted instructions substantially simultaneously
6 using a selected decryption algorithm to produce a plurality of decrypted instructions, wherein
7 said step of decrypting the plurality of encrypted instructions substantially simultaneously using
8 said selected decryption algorithm to produce said plurality of decrypted instructions comprises
9 the step of decrypting the plurality of encrypted instructions using at least one modified
10 decryption key, the at least one modified decryption key being formed responsive, at least partly,
11 to at least a portion of an address associated with at least one encrypted instruction of the
12 plurality of encrypted instructions; and

13 forwarding at least one decrypted instruction of the plurality of decrypted
14 instructions to a processing area of the processor.

1 7. (original) The method according to claim 6, wherein the at least one modified
2 decryption key is formed further responsive, at least partly, to at least one decryption key, the at
3 least one decryption key generated using at least a pseudo-random number generator.

1 8. (currently amended) A method for providing secure external memory that stores
2 instructions for a processor, comprising the steps of ~~The method according to claim 1, further~~
3 ~~comprising the steps of :~~

4 receiving a plurality of encrypted instructions into a buffer of the processor from
5 the external memory;

6 decrypting the plurality of encrypted instructions substantially simultaneously
7 using a selected decryption algorithm to produce a plurality of decrypted instructions;

8 transferring the plurality of decrypted instructions to another buffer; ~~and~~

9 forwarding at least one decrypted instruction of the plurality of decrypted
10 instructions to a processing area of the processor;

11 delaying said step of forwarding at least one decrypted instruction of the plurality
12 of decrypted instructions to a processing area of the processor until an instruction address
13 requested by the processing area corresponds to an instruction address associated with the at least
14 one decrypted instruction of the plurality of decrypted instructions; and

15 wherein said step of forwarding at least one decrypted instruction of the plurality
16 of decrypted instructions to a processing area of the processor comprises the step of forwarding

17 the at least one decrypted instruction of the plurality of decrypted instructions to the processing
18 area of the processor from the another buffer when the instruction address requested by the
19 processing area corresponds to the instruction address associated with the at least one decrypted
20 instruction of the plurality of decrypted instructions.

1 9. (original) The method according to claim 1, wherein the processing area of the
2 processor comprises at least one of a central processing unit (CPU) and an instruction decoder.

1 10. (original) The method according to claim 1, further comprising the step of:
2 forwarding the plurality of decrypted instructions to a cache of the processor.

1 11. (currently amended) ~~The method according to claim 1;~~ A method for providing secure
2 external memory that stores instructions for a processor, comprising the steps of:

3 receiving a plurality of encrypted instructions into a buffer of the processor from
4 the external memory;

5 decrypting the plurality of encrypted instructions substantially simultaneously
6 using a selected decryption algorithm to produce a plurality of decrypted instructions; and

7 forwarding at least one decrypted instruction of the plurality of decrypted
8 instructions to a processing area of the processor;

9 said ~~wherein~~ the method occurs within at least one of the following: a data
10 switcher or router; a subscriber line interface card; a modem; a digitally-controlled machining

11 tool; a portable radio; a wireless telephone; a voltmeter, ammeter, or ohmmeter; a personal
12 digital assistant (PDA); a television; a cable or satellite TV set top box; a camcorder; a piece of
13 audio/visual equipment; an audio compact disk (CD) system, player, or recorder; a digital
14 versatile disk (DVD) system, player, or recorder; a piece of financial equipment, including at
15 least one of a personal identification number (PIN) pad and a point of sale (POS) terminal; and a
16 smart card.

1 12. (original) A system for providing security to stored information, comprising:

2 at least one memory, said at least one memory storing a plurality of encrypted
3 instructions, each encrypted instruction of the plurality of encrypted instructions associated with
4 an address; and

5 a processor, said processor operatively coupled to said memory to retrieve the
6 plurality of encrypted instructions therefrom; said processor including:

7 a first buffer, the first buffer capable of receiving the plurality of encrypted
8 instructions;

9 a decryption unit, the decryption unit capable of receiving the plurality of
10 encrypted instructions from the first buffer, the decryption unit adapted to decrypt the plurality of
11 encrypted instructions using a decryption algorithm to produce a plurality of decrypted
12 instructions;

13 a second buffer, the second buffer capable of receiving the plurality of decrypted
14 instructions from the decryption unit; and

15 a processing area, the processing area capable of receiving at least one decrypted
16 instruction of the plurality of decrypted instructions.

1 13. (original) The system according to claim 12, wherein said processor comprises a
2 microcontroller.

1 14. (original) The system according to claim 12, wherein the processing area comprises at
2 least one of a central processing unit (CPU) and an instruction decoder.

1 15. (original) The system according to claim 12, wherein said processor further includes:
2 a cache memory, the cache memory capable of receiving the plurality of
3 decrypted instructions from the second buffer.

1 16. (original) The system according to claim 15, wherein the processing area is capable of
2 receiving the at least one decrypted instruction of the plurality of decrypted instructions from the
3 second buffer.

1 17. (original) The system according to claim 16, wherein said processor further includes:
2 a memory controller, the memory controller capable of controlling movement of
3 the plurality of decrypted instructions, the memory controller adapted to provide the processing
4 area the at least one decrypted instruction from the second buffer and to provide the cache the
5 plurality of decrypted instructions from the second buffer.

1 18. (original) The system according to claim 17, wherein the memory controller is further
2 adapted to provide the processing area the at least one decrypted instruction and the cache the
3 plurality of decrypted instructions substantially simultaneously.

1 19. (original) The system according to claim 17, wherein said processor further includes:
2 an address unit, the address unit capable of ascertaining a current instruction
3 address, the address unit adapted to provide the instruction address to the memory controller; and
4 wherein the at least one decrypted instruction is associated with an instruction
5 address "X" and another decrypted instruction of the plurality of decrypted instructions is
6 associated with an instruction address "X+1"; and the memory controller is further adapted to
7 provide the processing area the another decrypted instruction from the cache when the current
8 instruction address corresponds to the instruction address "X+1".

1 20. (original) The system according to claim 12, further comprising:
2 a bus, said bus operatively coupling said at least one memory to said processor;
3 and
4 wherein a width of said bus is equivalent to a width of each encrypted instruction
5 of the plurality of encrypted instructions.

1 21. (original) The system according to claim 20, wherein the width of said bus and the
2 width of each encrypted instruction is equal to eight (8) bits.

1 22. (original) The system according to claim 15, wherein the cache is a two-way, set
2 associative cache; and each block in each way of the cache is equal in length to a length of the
3 second buffer.

1 23. (original) The system according to claim 12, wherein the decryption unit is further
2 adapted to decrypt the plurality of encrypted instructions substantially simultaneously.

1 24. (original) The system according to claim 12, wherein the decryption algorithm
2 comprises at least one of a data encryption standard (DES), a triple DES, and an advanced
3 encryption standard (AES).

1 25. (original) The system according to claim 12, wherein the first buffer comprises a latch
2 that is capable of receiving the plurality of encrypted instructions sequentially directly from a bus
3 coupling said at least one memory to said processor.

1 26. (original) The system according to claim 12, wherein the system comprises at least
2 one of the following: a data switcher or router; a subscriber line interface card; a modem; a
3 digitally-controlled machining tool; a portable radio; a wireless telephone; a voltmeter, ammeter,
4 or ohmmeter; a personal digital assistant (PDA); a television; a cable or satellite TV set top box;
5 a camcorder; a piece of audio/visual equipment; an audio compact disk (CD) system, player, or
6 recorder; a digital versatile disk (DVD) system, player, or recorder; a piece of financial

7 equipment, including at least one of a personal identification number (PIN) pad and a point of
8 sale (POS) terminal; and a smart card.

1 27. (original) An arrangement for providing security to executable code stored in a
2 memory external to a processor, the arrangement comprising:

3 memory means, said memory means storing a plurality of consecutive encrypted
4 instructions;

5 means for sequentially receiving the plurality of consecutive encrypted
6 instructions into a buffer means;

7 means for substantially simultaneously decrypting the plurality of consecutive
8 encrypted instructions to create a plurality of consecutive decrypted instructions; and

9 means for distributing the plurality of consecutive decrypted instructions within
10 the processor when requested by a processing entity.

1 28. (original) The arrangement according to claim 27, wherein said means for distributing
2 the plurality of consecutive decrypted instructions within the processor when requested by a
3 processing entity includes means for transferring a decrypted instruction of the plurality of
4 consecutive decrypted instructions to the processing entity when the processing entity presents
5 an instruction address that is associated with the decrypted instruction.

1 29. (original) The arrangement according to claim 28, further comprising:

2 cache means, said cache means for storing decrypted instructions; and

3 wherein said means for distributing the plurality of consecutive decrypted
4 instructions within the processor when requested by a processing entity includes means,
5 responsive to a processing entity request, for transferring the decrypted instruction from said
6 cache means if the decrypted instruction is located therein upon receiving the processing request
7 or for transferring the decrypted instruction prior to storing the decrypted instruction in said
8 cache means if the decrypted instruction is not located therein upon receiving the processing
9 entity request.

1 30. (original) The arrangement according to claim 27, wherein the processor comprises a
2 microcontroller.

1 31. (original) The arrangement according to claim 30, wherein the microcontroller is
2 compatible with the 8-bit "8051" instruction set.

1 32. (original) The arrangement according to claim 27, wherein the arrangement
2 comprises at least one of the following: a data switcher or router; a subscriber line interface card;
3 a modem; a digitally-controlled machining tool; a portable radio; a wireless telephone; a
4 voltmeter, ammeter, or ohmmeter; a personal digital assistant (PDA); a television; a cable or
5 satellite TV set top box; a camcorder; a piece of audio/visual equipment; an audio compact disk
6 (CD) system, player, or recorder; a digital versatile disk (DVD) system, player, or recorder; a
7 piece of financial equipment, including at least one of a personal identification number (PIN) pad
8 and a point of sale (POS) terminal; and a smart card.

1 33. (original) The system according to claim 12, wherein the decryption unit is further
2 adapted to decrypt the plurality of encrypted instructions using a decryption key formed
3 responsive, at least partly, to at least a portion of the address associated with at least one
4 encrypted instruction of the plurality of encrypted instructions.

1 34. (original) The system according to claim 33, wherein:
2 the at least a portion of the address associated with at least one encrypted
3 instruction of the plurality of encrypted instructions comprises an address value; and
4 the decryption unit is further adapted to form the decryption key by utilizing at
5 least one of the following operations: (i) “xor”ing the address value with the decryption key, (ii)
6 adding the address value to the decryption key, and (iii) applying at least one of the address value
7 and the decryption key to a non-linear operation.

1 35. (original) The arrangement according to claim 27, wherein said means for
2 substantially simultaneously decrypting the plurality of consecutive encrypted instructions to
3 create a plurality of consecutive decrypted instructions includes at least one decryption key; and
4 wherein said arrangement further comprises:
5 means for creating the at least one decryption key using at least a portion of an
6 address associated with at least one encrypted instruction of the plurality of consecutive
7 encrypted instructions.

1 36. (original) The arrangement according to claim 27, wherein said memory means stores
2 a plurality of corresponding encrypted checksums; and

3 wherein said arrangement further comprises:

4 means for comparing a calculated checksum to a corresponding decrypted
5 checksum, the calculated checksum calculated from the plurality of consecutive decrypted
6 instructions, and the corresponding decrypted checksum decrypted with the plurality of
7 consecutive decrypted instructions from at least one corresponding encrypted checksum of the
8 plurality of corresponding encrypted checksums.

1 37. (original) The arrangement according to claim 36, wherein said arrangement further
2 comprises:

3 means for thwarting an attacker's attempts to breach security, said means for
4 thwarting an attacker's attempts to breach security becoming active when said means for
5 comparing a calculated checksum to a corresponding decrypted checksum determines that the
6 calculated checksum is not equivalent to the corresponding decrypted checksum.

1 38. (original) An arrangement for providing information security with a processor, the
2 arrangement comprising:

3 an encrypted buffer, said encrypted buffer capable of accepting a plurality of
4 encrypted units and adapted to offer the plurality of encrypted units;

5 a decryptor, said decryptor capable of accepting the plurality of encrypted units
6 and adapted (i) to decrypt the plurality of encrypted units to produce a plurality of decrypted
7 units and (ii) to offer the plurality of decrypted units;

8 a decrypted buffer, said decrypted buffer capable of accepting the plurality of
9 decrypted units and adapted to offer at least one of a single decrypted-buffer-originated
10 decrypted unit of the plurality of decrypted units and the plurality of decrypted units;

11 a cache, said cache capable of accepting the plurality of decrypted units and
12 adapted to offer a single cache-originated unit of the plurality of decrypted units;

13 a processing area, said processing area capable of accepting a decrypted unit of
14 the plurality of decrypted units and adapted (i) to ascertain a program address and (ii) to offer the
15 program address;

16 a controller, said controller capable of accepting the program address and adapted
17 to control movement of the plurality of decrypted units; and

18 wherein said controller, at least partially, causes (i) said cache to offer the single
19 cache-originated decrypted unit to said processing area if a first address associated with the
20 single cache-originated decrypted unit corresponds to the program address and (ii) said decrypted
21 buffer to offer the single decrypted-buffer-originated decrypted unit to said processing area and
22 the plurality of decrypted units to said cache if a second address associated with the single
23 decrypted-buffer-originated decrypted unit corresponds to the program address.

1 39. (original) The arrangement according to claim 38, wherein the arrangement
2 comprises at least one of the following: a data switcher or router; a subscriber line interface
3 card; a modem; a digitally-controlled machining tool; a portable radio; a wireless telephone; a
4 voltmeter, ammeter, or ohmmeter; a personal digital assistant (PDA); a television; a cable or
5 satellite TV set top box; a camcorder; a piece of audio/visual equipment; an audio compact disk
6 (CD) system, player, or recorder; a digital versatile disk (DVD) system, player, or recorder; a
7 piece of financial equipment, including at least one of a personal identification number (PIN) pad
8 and a point of sale (POS) terminal; and a smart card.

1 40. (original) The arrangement according to claim 38, wherein each unit comprises an
2 instruction.

1 41. (original) The arrangement according to claim 40, wherein each unit comprises a
2 byte.

1 42. (original) The arrangement according to claim 38, wherein a first length of a block of
2 said cache is equivalent to a second length of the plurality of decrypted units.

1 43. (original) The arrangement according to claim 38, wherein said decryptor is further
2 adapted to decrypt the plurality of encrypted units to produce a plurality of decrypted units using
3 at least one decryption key.

1 44. (original) The arrangement according to claim 43, wherein the at least one decryption
2 key is created, at least partially, responsive to at least a portion of the second address.

1 45. (original) The arrangement according to claim 38, wherein the plurality of encrypted
2 units and the plurality of decrypted units each comprise eight (8) bytes.

1 46. (original) A method for providing enhanced security for a processor, comprising the
2 steps of:

3 comparing a program address to at least one tag address of a cache to determine
4 whether there is a hit;

5 if the hit is determined, then transferring at least one information unit from the
6 cache to a processing area;

7 comparing the program address to an address corresponding to a decrypted buffer
8 to determine whether there is a decrypted buffer match;

9 if the hit is not determined and the decrypted buffer match exists, then transferring
10 another at least one information unit from the decrypted buffer to the processing area and
11 transferring a plurality of information units from the decrypted buffer to the cache;

12 comparing the program address to an address corresponding to a decryption unit
13 to determine whether there is a decryption unit match;

14 if the hit is not determined and the decrypted buffer match does not exist and the
15 decryption unit match does exist, then decrypting another plurality of information units in the

16 decryption unit and thereafter transferring the another plurality of information units from the
17 decryption unit to the decrypted buffer and transferring yet another at least one information unit
18 from the decrypted buffer to the processing area and transferring the another plurality of
19 information units from the decrypted buffer to the cache.

1 47. (original) The method according to claim 46, further comprising the steps of:
2 comparing the program address to an address corresponding to an encrypted
3 buffer to determine whether there is an encrypted buffer match;
4 if the hit is not determined and the decrypted buffer match does not exist and the
5 decryption unit match does not exist and the encrypted buffer match does exist, then transferring
6 yet another plurality of information units from the encrypted buffer to the decryption unit and
7 decrypting the yet another plurality of information units in the decryption unit and thereafter
8 transferring the yet another plurality of information units from the decryption unit to the
9 decrypted buffer and transferring still yet another at least one information unit from the
10 decrypted buffer to the processing area and transferring the yet another plurality of information
11 units from the decrypted buffer to the cache.

1 48. (original) The method according to claim 46, wherein the method occurs within at
2 least one of the following: a data switcher or router; a subscriber line interface card; a modem; a
3 digitally-controlled machining tool; a portable radio; a wireless telephone; a voltmeter, ammeter,
4 or ohmmeter; a personal digital assistant (PDA); a television; a cable or satellite TV set top box;

5 a camcorder; a piece of audio/visual equipment; an audio compact disk (CD) system, player, or
6 recorder; a digital versatile disk (DVD) system, player, or recorder; a piece of financial
7 equipment, including at least one of a personal identification number (PIN) pad and a point of
8 sale (POS) terminal; and a smart card.

1 49. (original) The arrangement according to claim 27, wherein said memory means stores
2 a plurality of corresponding checksums; and

3 wherein said arrangement further comprises:

4 means for comparing a calculated checksum to a corresponding checksum
5 of the plurality of checksums, the calculated checksum calculated from the plurality of
6 consecutive decrypted instructions, and the corresponding checksum is retrieved from said
7 memory means in which it is stored clear and unencrypted.

1 50. (original) A method for providing enhanced security for a processor, comprising the
2 steps of:

3 ascertaining a program counter;

4 determining whether an instruction associated with an address that corresponds to
5 the program counter is in a cache, a decrypted buffer, a decryption unit, or an encrypted buffer;

6 if so, forwarding the instruction;

7 if not,

8 retrieving a plurality of encrypted instructions from an external memory and
9 loading the plurality of encrypted instructions into the encrypted buffer, the plurality of
10 encrypted instructions including the instruction in an encrypted format;

11 forwarding the plurality of encrypted instructions from the encrypted buffer to the
12 decryption unit;

13 decrypted the plurality of encrypted instructions in the decryption unit to produce
14 a plurality of decrypted instructions, the plurality of decrypted instructions including the
15 instruction in an unencrypted format;

16 forwarding the plurality of decrypted instructions from the decryption unit to the
17 decrypted buffer; and

18 forwarding the instruction from the decrypted buffer for further processing.

1 51. (original) The method according to claim 50, further comprising the step of:

2 forwarding the plurality of decrypted instructions from the decrypted buffer to the
3 cache approximately during effectuation of said step of forwarding the instruction from the
4 decrypted buffer for further processing.